REMARKS

The above amendment and these remarks are responsive to the Office action of 30 Dec 2005 of Examiner Linh L.D. Son.

Claims 1-22 are in the case, none as yet allowed.

35 U.S.C. 101

Claims 8, 9, and 10 have been rejected under 35 U.S.C. 101.

The Examiner finds that the claimed invention is directed to non-statutory subject matter, stating:

> "Claims 8-10 recites a method for allowing the definition and configuration of NAT. The policy configuration and IP address pool configuration does not produce a 'useful, concrete and tangible result."

Applicants have amended claim 8, and thereby claims 9 and 10 which depend therefrom, to clarify the useful, concrete and tangible result to which the invention is directed: the processing of inbound and outbound packets.

Applicants request that claims 8-10 be allowed.

35 U.S.C. 103

Claims 1, 12, 13-16, 18, 19, 20 and 22) have been rejected under 35 U.S.C. 103(a) over Borella et al (U.S. Patent 6,353,614, hereinafter Borella) in view of Jain et al. (U.S. Patent 6,047,325, hereinafter Jain).

Claims 2-7 have been rejected under 35 U.S.C. 103(a) over Borella et al in view of Jain et al, and further in view of Arrow (U.S. Patent 6,226,751).

Claim 11 is rejected under 35 U.S.C. 103(a) over Arrow.

Claims 8-11, 17 and 21 have been rejected under 35 U.S.C. 103(a) over Allied Telesyn, NAT, GRE, and Security Associations, May 1998, Page 1-5, hereinafter "AT".

Applicants have amended these claims to clarify distinctions with respect to the cited art combinations. In so doing, applicants observe that in each case the additional clarifications are merely making explicit that which is understood by those of ordinary skill in the art as inherent in the VPN NAT technology of the invention when compared to the different technologies cited against the claims.

By way of background to various features of the claims, applicants invention relates in general to a technology involving IP security in a virtual private network (VPN) using network address translation (NAT) by performing one or a combination of the four types of VPN NAT, including

1. VPN NAT type 'a source-outbound' IP NAT,

2. VPN NAT 'b destination-outbound',

3. VPN NAT type 'c inbound-source' IP NAT, and

4. VPN NAT type 'd inbound-destination' IP NAT.

This involves dynamically generating NAT rules and associating them with manually or dynamically generated (IKE) Security Associations, before beginning IP security that uses the Security Associations. Then, as IP Sec is performed on outbound and inbound datagrams, the NAT function is also performed.

These 4 types of VPN NAT are defined in the specification at page 17, lines 5-19 (Table 2).

By using the current invention, one is given the ability to define and process multiple VPN NAT rules for a single VPN connection, via the specification of multiple IP addresses (an IP address set) for types of VPN NAT. The term 'VPN' here is used as a synonym for the IP Security protocols ESP (Encapsulating Security Payload) and AH (Authentication Header). Basic references for these protocols are (all from IETF (Internet Engineering Task Force)); IKE RFC2409 , ESP RFC2406, AH RFC2402, and the most basic, on IP Security architecture, RFC2401.

Of course, the subject invention works over local area networks (LANs) and wide area networks (WANs), including wireless; it works wherever IP traffic works. And is embodied in only one end of the VPN connection; the VPN implementation at the other end is completely unaware that its peer is performing VPN NAT operations. Even so, it may be embodied in both ends concurrently and independently, and this is a feature of the current invention. Applicants have amended the body of the claims to explicitly set forth this concept, previously set forth in preambles, and request that the Examiner now give patentable weight to it.

The problem addressed by the current invention is that IP Sec & NAT are conflicting; a packet with IP Sec applied cannot, in any way, be altered without invalidating the packet. Yet NAT requires that parts of a packet be altered. How can these technologies be made to function together in an integrated fashion, so that the benefits of each can be concurrently obtained?

One key idea (see, for example, claims 5-7) that allows integration of VPN & NAT is that the NAT operation is logically performed prior to beginning the IKE negotiation of Security Associations, and is integrated with the start of IKE negotiations. Hence the IKE negotiation begins and proceeds with the NAT IP address(es), rather than actual IP address(es), and no additional steps or devices are required. Hence any possible IP Sec protocol that is applied to a datagram (encryption or digital signature or both) works at both ends, because both IKE (and the resulting Security Associations) & IPsec are using the NAT address(es).

Following is a summary of how the present invention differs from cited prior art, as variously combined, in 6,353,614 (Borella et al), 6,047,325 (Jain et al), 6,226,751 B1 (Arrow et al), and AT (Allied Telesyn, configuration directions, 9 pages, for their 'software release 7.6, revisions 2, May 1998).

Borella describes a method and protocol for Distributed NAT ("DNAT") used to overcome the limited 32-bit address space of IPv4. The protocol includes a port allocation protocol and translates ports as well as IP addresses. Local ports are replaced with globally unique ports, unique for the scope of DNAT. Hence, Borella et al employs what is often referred to as 'PNAT', meaning 'port & network [IP] address translation'. The problems Borella addresses are those seen as inherent in the current versions of NAT (Col. 1, lines 41-67, Col. 2, lines 1-28).

So, some of the differences between Borella et al the subject invention are:

1) The subject invention does not translate ports (transport layer 'address') at all. The reason this is undesirable is because some classes of important IP traffic do use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast, VPN NAT handles all IP protocol traffic.

2) DNAT is a form of PNAT that centralizes the assignment and allocation of ports. Borella has nothing to do with IP Security or the IP Security protocols ESP & AH, nor with IKE. This is critical since the incompatibilities and difficulties of combining of IP Security & NAT are well known (see, for example, IETF RFC3715). Hence Borella et al does not even begin to address any of the problems associated with integrating IP Security and NAT. Nor is it a problem Borella is trying to solve.

3) The current invention does not use PAP (Port Allocation Protocol) (Col. 5, lines 61-62) or anything similar to PAP. The current invention does not allocate ports at

all, using anything.

4) Borella does not use or integrate VPN's (IP Sec-based or otherwise), whereas for the current invention, this is central. Borella does mention VPNs once (Col. 16, lines 20-23), but this in is merely an assertion. No description is given, no details, no elaboration. This single sentence does not anticipate, nor does it solve, the problems associated with using and integrating NAT with IP Sec-based VPNs.

So, Borella is directed to DNAT [see Col. 16, lines 7-23], not NAT, and requires processing both ends of the connection. And, of course, the present invention is not about NAT either, but rather is about VPN NAT.

Constant Port Values

In order to make even more clear the distinction between Borella (DNAT), and applicants' invention (VPN NAT), the independent claims have been amended to qualify NAT everywhere it is used with VPN, and by specifying, in claims 1, 12, 16, 18, 19, 20, and 22 that VPN NAT is applied to the datagram 'with source and destination port values after the application of VPN NAT being the same as before application of VPN NAT'. Of course, this later limitation is really what VPN NAT requires: the definition of VPN NAT includes not changing port values.

Applicants specification describes the above concept of constant port values. For example, Figures 5, 6 and 7 show how the VPN NATs work and they all show that ports are not changed.

Jain describes a network device which translates addresses and ports and filters packets at the link, network and transport layers. The invention uses a table (one of three mentioned) to bind MAC and IP addresses, via ARP (Address Resolution Protocol). Jain does say that traffic can be encrypted and authenticated when the traffic is sent over a wide-area-network. The problem Jain addresses is enabling a scalable virtual LAN (aka 'VLAN') over physical LANs and WANs.

Some differences between Jain and the subject invention are:

1) The current invention does not translate ports

(transport layer 'address') at all. The reason this is undesirable is because some classes of important IP traffic do not use TCP or UDP, hence the datagrams have no port numbers. These cannot be handled via a PNAT scheme. In contrast, VPN NAT handles all IP protocol traffic.

2) The current invention does not translate IP address based on MAC addresses as does Jain, nor does it map IP addresses based on MAC addresses (at all) (Col. 6, lines 29-32).

3) The current invention does not use ARP, and does not use MAC addresses at all. Hence the current invention solves the functional combination of IPsec-based VPN and NAT in a manner completely different from Jain (if Jain solves it). This is illustrated by the observation that both ends of Jain (Figure 1, elements 26 & 28) must embody Jain, while for the subject invention, brought out in all of applicant's claims as presently amended, only one end of the peer VPN connection embodies the subject invention.

4) The mapping of MAC addresses to IP addresses to change

apparent physical location of a IP address is the basic technology of VLANs. "If the packet is to be directed to a wide areas network, encryption and authentication procedures can be provided..." (Col. 2, lines 14-16). This and other passages in Jain suggest the relationship of Jain's use of VPN and Jain's use of network address translation (see for example important detail in Col. 5, lines 24-39). Note that first the packet is unencapsulated (a term commonly used in the context of VPN's) and then later (apparently optionally), a mapping to new MAC is made. In contrast, in the current invention, NAT is integrated with IP Sec.

5) Jain does not use IKE to automatically generate security associations.

However, with respect to claims 1, 12, 13-16, 18, 19, 20, and 22, the Examiner asserts that Jain teaches the VPN connection set up utilizing DHCP.

Applicants traverse. This is not what Jain does, and even if it were it does not teach the present invention.

Jain at Col. 5, lines 13-39 does not 'teach VPN connection setup utilizing the DHCP'. What Jain uses DHCP for is, is the same thing everyone that uses DHCP uses it for, which is what it was designed to do. And it simply does not do VPN connection setup. What Jain states (Col. 5, lines 19-25) is:

> "Additional security may be provided by binding machines to both MAC and IP addresses and having filters that check both the MAC and IP address of a source of a message. Such binding may be performed using domain name servers (DNS) and... DHCP."

Applicants argue that this must be distinguished from the current invention in many ways. The fact that at a later step of Fig. 7 a packet is 'unencrypted and decapsulated' (Col. 5, line 29) is distinguished from applicant's claims for the reason that this is clearly after the use of DHCP. Thus, Jain is not setting up a VPN connection, the phrase 'additional security' does not refer to IP Sec, VPN security associations or anything related to it. Thus, the binding of the MAC and an IP with DHCP or DNS or both does not teach applicant's claimed invention.

Same-system IP Address Data

In order to clarify the above distinction in the claims, applicants have amended the claims to specify the concept of 'same-system IP address data'. This refers to the VPN NAT address pools shown in Figure 2 and which are described at pages 15 and 16. See, for example, claim 1, which now states:

> "...configuring a VPN NAT IP address pool on a VPN gateway machine at said one end of a VPN connection employing only IP address data available at said VPN gateway machine..."

With respect to claim 11, the Examiner cites Arrow, and apparently equates SNMP and journal records. However, they are not the same.

Arrow describes how a selection of a plurality of (network) entities are coupled to a public data network. The plurality is given identifiers. VPN's can be set up among the plurality that include encryption & authentication & compression. "Another variation on the embodiment includes defining address translation rules for virtual private network units coupled to the public data network" (abstract). The purpose if Arrow is to enable the realization of virtual private networks.

Journal Records

Applicants have amended claim 11 to set forth that journal records are generated <u>as a log entry in a file system of an operating system at said one end of said VPN connection</u>. This is what journal records are, and SNMP is not. Support for this feature is found in applicant's specification at the bottom of page 13 to the beginning of page 14, where generating journal records is identified with logging.

With respect to claims 8-11, 17 and 21, the Examiner cites Allied Telesyn, NAT, GRE, and Security Associations, May 1998, pages 1-5, hereinafter 'AT'. These pages are configuration instructions for some device, and have the headings of 'Configuration Example 3' and 'NAT and security associations'. Both sections (chapters?) contain numbered lists of configuration instructions for connecting (see the two very similar diagrams) two LANs via two routers both connected to the Internet. The configuration instructions are for each router for each LAN.

Some key differences between the current invention and AT are:

1) The current invention uses IKE to automatically generate the security associations (this is shown in the current invention claim 1 "... based on IP Sec...") and AT does not. This is clearly shown in AT configuration instructions steps 11-14 for "Router A", 11-14 for "Router B", in the two boxes in the 'NAT and security associations' section (see the line "Manager > create enc key=1 val=random"), in steps 7-10 on the following page for another "Router A", and finally in steps 7-10 for "Router B" on the last page. Note, for example, back in the "NAT and security associations' section 2nd page, the paragraph under subheading "Instructions" where it says "... these keys must be created manually by typing a sequence of commands on a terminal ...". Quite clearly, these security association keys are manual and not created by IKE.

2) Another difference is that the NAT rule is created automatically in the current invention and in AT it is

created manually. Again, this can be clearly seen in steps 15-16 for "Router A" and 15-16 for "Router B".

3) The current invention only requires use of VPN NAT at a single end (see for example current invention claims 1, 8 and 11 all of which specify the claim "... at one end ...") of the VPN connection, while the AT document clearly does not. AT requires configuration at both ends. This is see in the configuration of Router A and Router B.

To more clearly set forth the above distinction, applicants have amended each of these claims to clarify in the claim body the feature of executing VPN NAT at one end of the connection.

Applicants are aware that a response to a 103 rejection combining references may not be adequate if the several references are distinguished without considering their combination. In this case, applicants argue that the distinctions, some (including same-system IP address data, generating journal records via I/O, and constant port values) clarified by amendments introduced to the claims herein, with respect to the several references render them incapable of combination in a proper manner to establish a prima facie case under section 103 of the patent statute.

Applicants request, therefore, that the rejection of claims 1-22 under 35 U.S.C. 103 be reconsidered and withdrawn.

SUMMARY AND CONCLUSION

Applicants urge that the above amendments be entered and the case passed to issue with claims 1-22.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

E. B. Boden, et al.

By

Shelley M Beckstrand

Shelley M Beckstrand
Reg. No. 24,886

Date: 28 Mar 2006

Shelley M Beckstrand, P.C.
Patent Attorney
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: (276) 238-1972
Fax: (276) 238-1545